EXPRESS MAIL EL121359825US

PAPER-BASED CONTROL OF COMPUTER SYSTEMS

Related Application Data

This application is a continuation-in-part of co-pending application 09/130,624, filed August 6, 1998, which is a continuation of application 08/508,083 (now Patent 5,841,978).

The subject matter of this application is generally related to that in all of the assignee's other patents and applications, e.g., patents 5,841,886, 5,832,119, 5,822,446 and 5,841,978, and the application entitled Methods and Systems Employing Digital Watermarking, filed on even date herewith.

Field of the Invention

The present invention relates to use of printed documents to control computer systems. Exemplary documents include business cards, advertisements, and identification badges, but the invention is not so limited.

Background and Summary of the Invention

Over the past century, business cards have formed part of business ritual. Functionally, they serve as a record of an encounter, and detail means by which the giver may be contacted (address, phone, etc.).

Business cards have changed, essentially, not at all in response to the advent of computers. Some accommodation has been made for business cards on the computer side, in the form of specialized scanner and optical character recognition tools by which textual data printed on cards can be read and entered into personal productivity software tools (e.g. contact managers, address books, datebooks, personal information managers, etc.). However, the data transferred into the personal productivity software is static and unchanging.

In accordance with one embodiment of the present invention, the textual information on a business card is supplemented with steganographically-encoded, multi-bit binary data. This latter data does not significantly distract from the visual aesthetics of the card (as would a bar code or the like), yet can be used by an associated computer to initiate a link to an internet site corresponding to the business card giver. At the site, the recipient of the card may gain access to the giver's schedule, and other information that changes over

time. (Such information may not generally be available over the internet to persons without the card data.)

The foregoing and additional features and advantages of the present invention will be more readily apparent from the following detailed description, which proceeds with reference to the accompanying drawings.

Brief Description of the Drawings

Fig. 1 shows a flow chart of a process according to one embodiment of the present invention.

Detailed Description

Digital watermarking is a quickly-growing field of endeavor, and many techniques are known. Generally, all seek to steganographically convey multi-bit data ancillary to some other signal or medium.

The present assignee's prior application 09/127,502, filed July 31, 1998, shows techniques by which very fine lines can be printed on a medium to slightly change the medium's apparent tint, while also conveying digital data. Commonly-owned application 09/074,034, filed May 6, 1998, details how the contours of printed imagery can be adjusted to convey digital data. (That technique can be applied to printed text characters, as well as the line art imagery particularly considered.) Applicant's patent 5,850,481 details how the surface of paper or other media can be textured to convey optically-detectable binary data. Applicant's patents 5,841,886, 5,809,160, and the priority applications detailed above, detail various techniques for steganographically encoding photographs and other imagery.

Three papers by Brassil et al show other techniques for conveying watermark data by slight changes to printed text, "Electronic Marking and Identification Techniques to Discourage Document Copying," Proceedings of INFOCOM '94 Conference on Computer, IEEE Comm. Soc Conference, June 12-16, 1994, pp. 1278-1287; "Hiding Information in Document Images," November, 1995, 7 pages, AT&T Bell Laboratories Technical Report (available at ciss95_ps.z from ftp://ftp.research.att.com/ dist/ brassil/ 1995/ ciss95.ps.Z.; and "Document Marking and Identification using Both Line and Word Shifting," INFOCOM '95 (available at ftp://ftp.research.att.com/ dist/ brassil/ 1995/ infocom95.ps.Z).

The foregoing is just a sampling of the large literature on watermarking. The artisan is presumed to be familiar with such art, all of which is generally suitable for use with the novel concepts detailed below.

In accordance with any of the known watermarking techniques, a business card is steganographically encoded with plural bit data. At least part of this data identifies an internet address or web site at which data about the giver of the card is stored. If sufficient bits can be encoded into the business card, the address can be encoded literally, e.g., by ASCII or binary numeric encoding. Alternatively, to reduce the data payload, an abbreviated form of address. One example of such an abbreviated form is a Unique Identifier (UID) which can be, e.g., a 24-bit value.

Desirably, the steganographic encoding is tailored to facilitate decoding in the presence of arbitrary rotation or scale distortion of the card introduced during scanning. (Some such techniques are shown, e.g., in applicant's related patents identified above. Others are known to artisans.)

As shown in Fig. 1, the card is scanned (e.g., by use of conventional opto-electronic devices, such as a scanner or a digital camera). The output data is then optionally processed to account for any skew or scale factor. The plural-bit digital data is then decoded and stored, e.g., in personal productivity software.

(Although not particularly shown in Fig. 1, it is expected that the detailed process will often be supplemental to known OCR-reading of business cards, and entry of the textual data into personal productivity software. That is, the scan data is processed both by OCR techniques, and by steganographic decoding techniques, and the results of both operations stored in a data structure or other memory for later reference.)

The steganographically-decoded plural-bit data is provided to a web browser or other internet appliance and used to initiate a link to a remote computer over the internet's network of computers. If the remote address was literally encoded in the business card, that address is used directly. If an abbreviated form of address was encoded, an additional step may be required.

If a UID was encoded in the card, rather than a literal address, the web browser might consult an index to correlate the UID to an address. The index could be a table or other data structure stored on the user's local computer, but more commonly is a remote name server

database to which the browser links as a default when processing business card UIDs. Data obtained from the index is then used to complete the linking to the ultimate destination. (In addition to reducing the business card payload, such linking through an index, e.g., by a UID, offers flexibility in that the ultimate destination can be moved to other server sites as needed, with just a simple update to the index. Alternatively, all business cards encoded with the former address would be rendered obsolete if the site were relocated.)

At the ultimate site, the user is presented with whatever information the business card giver chooses to provide, including biographical information, photos, promotional offers or advertisements relating to the card-giver's business (or relating to enterprises to whom the card-giver has rented screen space), etc., etc.. In one embodiment, the giver's site is linked to the giver's personal productivity tool(s) and permits viewing, e.g., of calendar information (showing where the business card giver is scheduled to be today, or for the rest of the week, month, etc.)

Typically, this calendar information is not available to casual web browsers; the steganographically decoded data from the business card includes some authentication data (akin to a password) that permits access to otherwise restricted data. This authentication data can take the form of a web page address to which no publicly-accessible link points, a password that is separately presented to the web server by the user's browser after a link is established, or other known technique.

In one form of the invention, the giver of business cards may have several differently-encoded cards, each with a different level of access authorization. Thus, some cards may access a biographical page without any calendar information, other cards may access the same or different page with access enabled to today's calendar, and still other cards may access the same or different page with access enabled for the card-giver's complete calendar.

The reference to business cards and personal calendars is illustrative only. The invention is more widely applicable. Going back a century, "calling cards" were used by persons whose interests were strictly social, rather than business. The principles of the present invention can similarly be applied. Teenagers can carry small cards that can be exchanged with new acquaintances to grant access to private dossiers of personal information, favorite music, artwork, video clips, etc. The cards can be decorated with art or other indicia

that can serve purposes wholly unrelated to the linking data steganographically encoded therein.

Even the "card" paradigm is too restrictive. The same techniques can be applied to any object. A music CD cover can be encoded to point to a promotional site associated with the music artist. A book jacket can link to a similar site. Printed advertising distributed through the US mail (cards, magazines, etc.) can be encoded to point to related web-based promotional sites. (Sponsors of such advertising or other sites can reward visits to their internet site by issuing visitors digital tokens or coupons that can be redeemed for premiums, cash-back, etc., either for any such visit, or only if the visit was effected through the portal of a steganographically-encoded printed medium.)

Many contexts arise in which data to be presented to a consumer is valuable only if timely. The postal service mail is ill-suited for some such information due to the latency between printing a document, and its ultimate delivery to a recipient. The principles of the present invention allow the recipient to take a steganographically-encoded data object (card, etc.) that was printed well before delivery, and use it on receipt to receive up-to-the-minute information. (In this and other embodiments, the steganographically-encoded data can also include data uniquely identifying the recipient/user, so the web site can present data customized to that user.)

The present technology also has application in access control systems. An identification badge (either with photo or graphics, or with text alone) can be encoded with steganographically access control data (e.g., access codes or digital keys) that is recognized by optical-scanner-equipped locks and the like, permitting access by authorized persons to restricted areas or restricted services (e.g., computer privileges). Given the low cost of media and printing (as compared with other access control technologies), the cards can be issued on a daily, weekly, or other frequent interval, and the access control system can be programmed to permit access in response to such cards only for the pre-set limited period. Lost cards soon lose their threat.

Tickets to sporting events, concerts, and other events can be steganographically encoded to permit the bearer to access premium web content available only to those who have purchased tickets (e.g., an on-line text-, audio-, or video-chat session with the featured performer or sports star the day before the event). Alternatively, the encoded data may link to

a transactional site. In some such embodiments, the ticket is printed with a nominal show data and seat assignment, but also includes a UID in addition to the encoded address of an associated transactional ticket site. The user then can visit the transactional web site to change seating (or date). On attending the event, the consumer presents the ticket to a steganographic decoder apparatus that discerns the UID and looks up the seat assignment most-recently picked by the consumer. It then prints a chit entitling the consumer to take the seat earlier selected on-line.

The reference to "scanning" of objects naturally brings to mind images of desktop flatbed scanners, or multi-function hydra devices. While such devices can be used -- together with convention digital cameras (including video cameras) -- the inventors foresee that image input devices will soon be much more commonplace. The provision of digital cameras as built-in components of certain computers (e.g., the Sony Vaio laptops) is just one manifestation of this trend. Another is camera-on-a-chip systems, as typified by U.S. Patent 5,841,126 and detailed in Nixon et al., "256x256 CMOS Active Pixel Sensor Camera-on-a-Chip," IEEE J. Solid-State Circuits, Vol. 31(12), pp. 2046-2051 (1996), and Fossum, "CMOS Image Sensors: Electronic Camera-on-a-Chip," IEEE Transactions of Electron Devices, vol. 44, No. 10, Oct. 1997. Still another is head-mounted cameras (as are presently used in some computer-augmented vision systems). These and other image input devices can all be used in connection with the present invention.

To facilitate embodiments of the present invention, a prior art camera-on-a-chip system can be modified to also include a steganographic watermark detector on the same semiconductor substrate. Such a chip – in addition to providing image output data – can also analyze the image data to discern any steganographically encoded data, and produce corresponding output data. (Again, such analysis desirably includes correction for scale and rotation factors, so precise positioning of the object being "read" is not essential for correct decoding.)

To provide a comprehensive disclosure without unduly lengthening this specification, applicants incorporate by reference the patents, applications, and publications identified above.

Having described an illustrated the principles of our invention with reference to illustrative embodiments, it should be recognized that the invention is not so limited.

For example, while certain of the embodiments were illustrated with reference to an internet-based embodiment, the same techniques are similarly applicable to any other computer-based system. Likewise, for internet-based embodiments, the use of web browsers and web pages is not essential; other digital navigation devices and other on-line data repositories can be similarly accessed.

In view of the many embodiments to which the principles of our invention may be applied, it should be recognized that the detailed embodiments are illustrative only and should not be taken as limiting the scope of our invention. Rather, we claim as our invention all such embodiments as fall within the scope and spirit of the following claims, and equivalents thereto.

WE CLAIM

1. A method comprising:

presenting a business card of an individual to an optical sensor, the optical sensor producing output data;

decoding steganographically-encoded plural-bit data from the sensor output data; and

using said plural-bit data to establish a link to an internet address having data relating to the proprietor of said business card.

2. The method of claim 1 which includes obtaining from said internet site calendar data detailing certain activities of the individual.

3. The method of claim 2 in which the amount of calendar data obtained depends on an authorization level.

4. The method of claim 3 in which the authorization level is reflected in the plural-bit data encoded in the individual's business card, wherein an individual can distribute differently-encoded cards to different recipients, to grant the recipients different access rights to said calendar data.

5. The method of claim 1 in which the optical sensor is a business card reader that also serves to input textual information from business cards into a personal information manager.

6. The method of claim 5 which includes storing an internet address discerned from the steganographically-encoded plural-bit data into said personal information manager.

7. The method of claim 1 in which the optical sensor is a digital camera.

8. The method of claim 7 in which the digital camera is mounted to a computer display device.

9. The method of claim 7 in which the digital camera is head-mounted on a user thereof.

10. A method comprising:

presenting a printed promotion to an optical sensor at a first site, the optical sensor producing output data;

decoding steganographically-encoded plural-bit data from the sensor output data;

using said data to establish a link to an internet site relating to a company, product, or service promoted by said printed promotion; and

transferring to from the internet site to the first site additional information relating to said company, product, or service.

11. A method comprising:

presenting a printed identification badge to an optical sensor, the optical sensor producing output data corresponding to optical characteristics of the face of said badge;

decoding steganographically-encoded plural-bit data from the sensor output data;

checking the plural-bit data to determine whether it corresponds to a valid access card; and

unlocking a lock depending on the outcome of the foregoing checking operation.